IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. BOGDAN NICOLESCU, et al. Defendant.	))))))))))	CASE NO. 1:16-CR-224 JUDGE PATRICIA A. GAUGHAN **UNITED STATES OF AMERICA'S OPPOSITION TO MICLAUS' MOTION IN LIMINE RE: TESTIMONIAL HEARSAY STATEMENTS**

Now comes the United States of America, by its counsel, Justin E. Herdman, United States Attorney, Duncan T. Brown and Brian M. McDonough, Assistant United States Attorneys, and Brian L. Levine, Senior Counsel for the U.S. Department of Justice, and hereby opposes Defendant Radu Miclaus' Motion In Limine Re: Testimonial Hearsay Statements.

INTRODUCTION

Miclaus' generic "produce everything early" motion is the solution to a problem that doesn't exist in this particular case. Contrary to Miclaus' motion (Dkt. 73 at 5), the United States does not intend to offer *any* testimonial hearsay statements in this case, nor does it intend to offer evidence pursuant to Federal Rule of Evidence ("FRE") 807 (the "residual exception"). Instead, as discussed in great detail below, virtually all of the "statements" offered by the government will be offered for non-hearsay purposes, and even if offered for the truth of the matter asserted, would be in furtherance of the conspiracy, and/or statements of a party opponent. FRE 801(d)(2)(A) & 801(d)(2)(E). Non-hearsay statements, co-conspirator statements, and statements of a party opponent do not implicate the Confrontation Clause. *See Crawford v. Washington*, 541 U.S. 36, 59 n. 9 (2004) (Confrontation Clause "does not bar the

use of testimonial statements for purposes other than establishing the truth of the matter asserted."); *United States v. Kenney*, 218 F. App'x 380, 385 (6th Cir. 2007) ("as non-hearsay the testimony does not implicate any Sixth Amendment concerns such as those raised in *Crawford v. Washington*").

Similarly, because the Court already addressed authentication in a prior ruling (Dkt. 70) and because the United States plans to authenticate evidence not already approved by the Court primarily through live witness testimony and evidence of "distinctive characteristics" pursuant to FRE 901(b)(4), the United States does not anticipate Confrontation Clause issues related to authenticity.

Nor is the volume of discovery in this case an appropriate basis to deviate from the existing schedule because the United States has already been voluntarily providing defense with exhibits, virtually as they are created. Although Miclaus completely fails to mention it, when Miclaus recently asked the United States to produce its "greatest hits" list, the United States voluntarily produced several hundred pages of hard-copy documents representing what the United States had then-identified as its most significant exhibits. The entire prosecution team then met personally with Miclaus and his counsel to review these documents for several hours. Since that meeting, the United States has continued to cooperate with and produce likely exhibits to the defendants. In sum, Miclaus identifies no reason to deviate from the Court's pretrial order, and his motion should be denied.

ANALYSIS

I. THE GOVERNMENT HAS AND WILL CONTINUE TO PROVIDE DEFENDANTS WITH EARLY ACCESS TO EXHIBITS AND TO OPENLY RAISE EVIDENTIARY ISSUES.

From the beginning, the United States' approach in this case has been to: (a) accommodate defense requests; (b) provide defense with an unprecedented level of access to documents and information; (c) provide potential exhibits to defense shortly after they are created; and (d) openly raise evidentiary issues as early as possible. For example:

- At the December 2016 arraignments, the government began producing documents to the defendants, physically handing defense counsel key prosecution documents.

- Not long after arraignment, the government held a reverse proffer for all three defense counsel at the FBI's offices. During that meeting, the government presented many of its key documents and answered questions from defense counsel for several hours.

- Since arraignment, the government has produced or provided access to discovery on multiple occasions. In each instance, the government did not simply "drop" a large volume of documents on defense, but had detailed phone conversations with defense counsel, in which the government explained the contents and context for each production, and pointed defense counsel to the most significant documents in the production.

- On March 23, 2018, the government filed a "Notice Pursuant to Federal Rule of Evidence 801(d)(2)(E)" (Dkt. 58), in which it laid out its explanation of why the "statements" the government seeks to introduce "do not constitute hearsay" (*id.* at 2), but also provided notice of the intent to use the "co-conspirator" exception in an abundance of caution. (*Id.* at 3.) The United States attached to its notice approximately 70 pages of examples of such "statements." (Dkt. at 58-1.) No defendant filed any response or objection to the government's notice.

- April 9, 2018 was the Court's motion deadline. On that date, the government filed a "Motion in Limine Regarding Authentication," to obtain clarity on certain issues related to authentication and the Confrontation Clause. (Dkt. 60.) The United States attached to its Motion, approximately 264 pages of certificates from internet service providers (ISPs) and digital investigative analysts who imaged defendants' devices. (Dkt. 60-1.) Defendant Miclaus filed no response to the government's motion.

- On or about March 20, 2018**,** the prosecution team met with counsel for Miclaus, who requested that the government produce a collection of the exhibits constituting its "greatest hits," even though those records could be found amongst the discovery already produced or made available to defense.

- On or about April 11, 2018, the government provided Miclaus and his counsel with several hundred pages of documents constituting the "greatest hits" documents Miclaus' counsel had requested. That same day, the entire prosecution team also met with both Miclaus and his counsel for several hours to review the "greatest hits" documents and to answer any questions. Shortly thereafter, the government produced the same "greatest hits" documents to the other defendants as well.

- On May 31, 2018, the Court issued an Order granting, in part, the government's authentication motion. (Dkt. 70.) Where the Court did not find that a certificate was sufficient, the government intends to provide live witness testimony. To the extent the government obtains additional certificates related to authenticity, they will be produced soon after receipt. *See, e.g.*, **Exhibit A** (certificate from Afraid.org dated June 22, 2018).

- On June 23, 2018—two days before Miclaus filed his motion—the government wrote each of the defense counsel via letter and email noting, among other things, that "some of you requested the 'greatest hits,' so as the government continues to identify and prepare 'excerpts' or 'extracts' from the voluminous records it has already produced and/or made available to you, it is providing you with those excerpts or extracts in the interest of focusing your attention on the evidence that is the most likely to use during its case-in-chief." *See* **Exhibit B**.

- Nonetheless, two days later, on Sunday, June 25, 2018, Miclaus filed his motion.

In sum, while there is a large volume of digital evidence in this case, the government has consistently directed the defense to the records it is most likely to use in its case-in-chief, and has, at every opportunity, attempted to cooperate and simplify the case for defense.[1] The United

[1] Miclaus asserts that the government has produced "well over 8 terabytes" of digital information. (Dkt. 73 at 2 n.2). This figure is misleading for a variety of reasons. First, terabytes of this "digital information" simply reflected multiple image copies made of the Bayrob Groups' C&C Server. These images are mostly redundant with each other and the multiple redundant copies obtained from different providers is primarily offered to show that each copy is authentic. Second, some of this data is communications between Bayrob Members—the vast majority of which were encrypted and thus cannot be analyzed and can only be offered for the fact that the communications are encrypted. Third, much of this data represents a large volume of internet traffic intercepted by Romanian authorities, from which the government only intends to make a couple of points: (a) the defendants had daily encrypted communications with a Jabber and VOIP server that Danet controlled; and (b) the defendants visited cryptocurrency related websites from their homes and cellphones which related to the cryptocurrency mining they were doing through their Botnet. This is also a good example of how the government has and continues to direct defense directly to what is most relevant and

States will continue to do so. Miclaus has identified no basis for the Court to deviate from its usual pretrial order.

II. NO EVIDENTIARY ISSUE IN THIS CASE REQUIRES A DEPARTURE FROM THE PRETRIAL ORDER

Miclaus bases his demand for early production of exhibits largely on his misplaced speculation that the United States is planning to introduce "testimonial hearsay statements" and evidence pursuant to FRE 807—the so-called "residual exception"—which requires the movant to provide advanced notice to opposing parties. (Dkt. 73 at 5.) The United States, however, does not intend to offer any testimonial hearsay statements, and does not anticipate introducing evidence pursuant to FRE 807. To the contrary, virtually all of the evidence at issue in this case is non-hearsay, but even if it were hearsay, it would constitute statements of a party opponent or in furtherance of the conspiracy, and thus does not raise Confrontation Clause issues.

Similarly, where the Court did not already accept a certificate to authenticate records or images (Dkt. 70), the government plans to rely primarily on FRE 901(b)(4) (distinctive characteristics) and live witness testimony to authenticate the evidence. Thus, the United States does not foresee any difficult evidentiary issues that would necessitate deviating from the deadlines already set by the Court.

A. Confrontation Clause

As will be discussed Section II(B) ("Hearsay") below, all (or virtually all) of the "statements" presented by the United States will not be offered for the truth of the matter asserted, and thus will not constitute hearsay. The Confrontation Clause is not implicated by non-hearsay evidence. *See Crawford v. Washington*, 541 U.S. at 59 n. 9 (Confrontation Clause

---

material.

"does not bar the use of testimonial statements for purposes other than establishing the truth of the matter asserted."); *United States v. Kenney*, 218 F. App'x at 385 ("as non-hearsay the testimony does not implicate any Sixth Amendment concerns such as those raised in *Crawford v. Washington*").

With respect to the vast majority of these "statements," even if they were offered for the truth of the matter asserted, the statements would also be by a party opponent and in furtherance of the conspiracy. FRE 801(d)(2)(A), (E). Statements of a party opponent and statements in furtherance of the conspiracy also do not implicate the Confrontation Clause. *See United States v. Tragas*, 727 F.3d 610, 615 (6th Cir. 2013) ("statements made in furtherance of the conspiracy . . . were categorically non-testimonial and also within a 'firmly rooted' exception to the hearsay rule"); *United States v. Martinez*, 430 F.3d 317, 329 (6th Cir. 2005) (co-conspirator statements do not violate the Confrontation Clause); *United States v. Tolliver*, 454 F.3d 660, 665 (7th Cir. 2006) (statements of a party opponent do not constitute testimonial hearsay); *United States v. Hargrove*, 508 F.3d 445, 449 (7th Cir. 2007) (same).

While some of the records the United States may seek to introduce are business or public records, "[b]usiness and public records are generally admissible absent confrontation . . . because—having been created for the administration of an entity's affairs and not for the purpose of establishing or proving some fact at trial—they are not testimonial." *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 324 (2009); *United States v. Williams*, 662 F. App'x 366, 376 (6th Cir. 2016) ("the mere fact that a business record might foreseeably be relevant to a subsequent prosecution does not automatically transform the record into a 'testimonial' statement."); *Maurent v. Warden, Ross Corr. Inst.*, No. 2:14-CV-2296, 2016 WL 1436680, at *15 (S.D. Ohio

Apr. 11, 2016) (letter from the sheriff certifying that calls downloaded and transferred onto a CD were a true and accurate copy of petitioner's recorded calls from jail was not testimonial).

The only issue that the United States anticipates could implicate the Confrontation Clause is the use of certifications of authenticity. The Court, however, has already ruled on the United States' motion *in limine* on that topic. (Dkt. 70.) As discussed in great deal in Section II(C) ("Authentication") below, where the Court found that proffered certifications were insufficient, the United States plans to rely primarily on live witness testimony and the distinctive characteristics of each digital device or other piece of evidence to make a *prima facie* case that the evidence is what the government purports it to be. *See* FRE 901(b)(4) (party may authenticate evidence based on "the appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.") To the extent the United States obtains any additional certificates, that United States will produce those to defense as soon as practicable. *See* **Exhibit A**.

B. Hearsay

All or virtually all of the evidence the United States seeks to introduce in this case is non-hearsay, but even if considered hearsay, it would be a statement of a party opponent and in furtherance of the conspiracy.

1. <u>The United States Will Offer Primarily Non-Hearsay Evidence</u>

The evidence that the United States will offer in this case essentially falls into one of four category. The first category is evidence of the crime itself—the fraudulent statements the defendants made to trick victims into clicking on malicious attachments, providing personal information, sending money to the defendants, and/or serving as money mule. The second category is evidence to connect the individual defendants to their criminal monikers, and to

connect their criminal monikers to the crimes. The third category is evidence offered to help authenticate other evidence. The fourth category is victim statements offered to connect the criminal monikers to particular victims or to explain law enforcement's investigatory steps. All of this evidence will be offered for non-hearsay purposes.

Fraudulent Statements and Instructions. Many of the "statements" the government will offer are the fraudulent statements the Bayrob Group made in order to trick victims into clicking on malicious attachments, providing personal information, sending money to defendants, and/or serving as a money mule. *See, e.g.*, Dkt. 58-1 at Exhibits G-I. These "statements" will be offered as evidence of the fraud, itself. "When statements are offered to prove the falsity of the matter asserted, there is no need to assess the credibility of the declarant." *United States v. Thompson*, 501 F. App'x 347, 363 (6th Cir. 2012) (quoting *United States v. Hathaway*, 798 F.2d 902, 905 (6th Cir. 1986)). "Since there is no need to assess the credibility of the declarant of a false statement," there is "no purpose which would be served by extending the definition of hearsay to cover statements offered for the falsity of the matter asserted." *Id.* The Sixth Circuit has "therefore join[ed] those courts which have concluded that statements offered to prove the falsity of the matter asserted are not hearsay." *Id.*; *see also United States v. Ivory*, 875 F.2d 868 (6th Cir. 1989) ("Evidence of false representations on a tax return do not constitute hearsay because they are not offered to prove the truth of the matter asserted.")

Similarly, evidence of defendants' crime may include the defendants' malware, itself, and other commands or instructions the defendants programmed or entered into a web browser in aid of their crime. Because commands, orders, or instructions are not assertions capable of being true or false, they are non-hearsay as well. *See United States v. Rodriguez-Lopez*, 565 F.3d 312, 314–15 (6th Cir. 2009) ("if the statements were questions or commands, they could not—absent

some indication that the statements were actually code for something else—be offered for their truth because they would not be assertive speech at all. They would not assert a proposition that could be true or false."); *see also Blair v. Henry Filters, Inc.*, 505 F.3d 517, 524 (6th Cir. 2007) ("A statement offered as evidence of the bare fact that it was said, rather than for its truth, is not hearsay."); *United States v. White*, 639 F.3d 331, 337 (7th Cir. 2011) ("[A] command is not hearsay because it is not an assertion of fact."); *United States v. Robinzine*, 80 F.3d 246, 252 (7th Cir.1996) (holding that an order or request "could not be hearsay, since it made no assertion of fact that could be true or false");*United States v. Shepherd*, 739 F.2d 510, 514 (10th Cir. 1984) ("An order or instruction, is, by its nature, neither true nor false and thus cannot be offered for its truth.").

Other such evidence is not hearsay because it was "generated by a computer and thus was not a 'statement.'" *BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc.*, 881 F.3d 293, 313 (4th Cir. 2018) (copyright infringement notices generated by a computer are not "statements" and thus not hearsay); *United States v. Channon*, 2018 WL 627443 (10th Cir. 2018) (spreadsheets reflecting point-of-sale data were machine-generated records falling outside of the hearsay rule); *United States v. Moon*, 512 F.3d 359, 362 (7th Cir. 2008) ("[T]he instruments' [an infrared spectrometer and a gas chromatograph] readouts are not 'statements.'"); *United States v. Washington*, 498 F.3d 225, 230-31 (4th Cir. 2007) (printed result of computer-based test was not the statement of a person and thus would not be excluded as hearsay); *United States v. Hamilton*, 413 F.3d 1138, 1142-43 (10th Cir. 2005) (computer-generated header information was not hearsay as "there was neither a 'statement' nor a 'declarant' involved here within the meaning of Rule 801"); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) ("nothing 'said' by a machine . . . is hearsay") (quoting 4 Mueller & Kirkpatrick, *Federal Evidence* § 380, at 65 (2d

ed. 1994)); *Satmodo, LLC v. Whenever Commc'ns, LLC*, No. 3:17-CV-192-AJB-NLS, 2017 WL 4557214, at *2 (S.D. Cal. Oct. 12, 2017) (Google Earth records admissible because "the relevant assertion isn't made by a person; it's made by the Google Earth program."); 2 Kenneth S. Broun, et al., McCormick on Evidence § 294 (5th ed.1999) (classifying records that are self-generated by machine or computer as non-hearsay).

Evidence of Identity. The government will also offer evidence for purposes of either (a) connecting the individual defendants to their criminal monikers; and (b) connecting defendants' criminal monikers to the crimes. An example of evidence connecting the defendants to their criminal monikers is conversations between defendants in which they reference their criminal monikers or reference the names of files or folders on the Command and Control server which the Bayrob Group used to control the Botnet (the "C&C Server"). An example of evidence connecting the defendants' criminal monikers to the crime is references the defendants' criminal monikers on the C&C Server. All of these conversations have been previously disclosed to defense counsel.

In each of these examples, the government is not seeking to prove the truth of the matter asserted. As an example, in one chat conversation between two defendants (obtained from the Miami search of Danet's phone (Dkt. 71)), Danet writes Nicolescu that he fixed something stupid in "epoll." The government offers this statement for identity—the fact that both of these defendants were discussing "epoll"—a file on the C&C Server used to poll the Botnet—tends to establish their membership in the Bayrob Group. That is true regardless of whether or not something was actually "stupid" in epoll, and whether or not Danet actually fixed it.

Offering statements to establish the identity of the declarant or others referenced in or involved in the conversation is a non-hearsay purpose. In *United States v. Gaitan-Acevedo*, 148

F.3d 577 (6th Cir. 1998), the government offered phone numbers and addresses from a drug ledger to demonstrate that members of the conspiracy associated with each other for business purposes. The defendants contended that the evidence was offered for the truth of the matter asserted, and thus, inadmissible hearsay. The Sixth Circuit disagreed, finding that "[p]ersonal telephone directories and notebooks are admissible . . . for non-hearsay purposes of showing that *a conspiracy existed and that a defendant was a member of the conspiracy*." *Id.* at 591 (emphasis added). The Court explained that "[t]hese documents are not offered to prove the information they contained and therefore, may not be excluded as hearsay." *Id.*; *see also United States v. Munguia*, 273 F. App'x 517, 521 (6th Cir. 2008) (relying on *Gaitan-Acevedo*).

To return to the earlier example, here, the fact that a defendant referenced "epoll" in a conversation will be offered "as evidence of the bare fact that it was said, rather than for its truth" and is therefore not hearsay. *Henry Filters, Inc.*, 505 F.3d at 524; *Gaitan-Acevedo*, 148 F.3d at 591; *see also United States v. Mazyak*, 650 F.2d 788, 792 (5th Cir. 1981) ("The government offered the letter for the limited purpose of linking the appellants with the vessel and with one another. The use of the letter for this limited purpose was not hearsay. The letter was not introduced to prove the truth of the matter asserted; rather, it was introduced as circumstantial proof that the appellants were associated with each other and the boat.")

Authentication Evidence. Similarly, the government will offer certain statements merely for the purposes of authenticating evidence. For example, the government may offer a series of emails found on one defendant's cellphone or computer simply to show that the cellphone or computer belonged to and was controlled by the defendant sending and receiving the emails. *See, e.g., United States v. Koch*, 625 F.3d 470, 479 (8th Cir. 2010) (fact that documents authored by "Jonathan Koch" as well as user names "Jo" and "Jonathon" were found

on a computer and flash drive were not offered for the truth of the matter asserted but to connect the defendant to the devices); *see also United States v. Manning*, 738 F.3d 937, 943 (8th Cir. 2014) (chats were not hearsay because they were "circumstantial evidence connecting [defendant] to the child pornography on the computer and [to] the Memorex disc discovered near the computer"); *United States v. Pulido-Jacobo*, 377 F.3d 1124, 1132 (10th Cir. 2004) (finding a receipt to be admissible non-hearsay because "the government offered the engine receipts only to show that [defendant] had sufficient control of the car to store an old receipt in it"); *Mazyak*, 650 F.2d at 792 (letter was not hearsay where it was offered "for the limited purpose of linking the appellants with the vessel and with one another.")

Victim Statements. The government may introduce statements from victims for purposes other than the truth of the matter asserted. Some of the victim statements will be offered merely to connect the defendants to particular crimes because the victim statements were either (a) stored on the C&C Server or (b) connected to specific communications between Bayrob Group members. *See Gaitan-Acevedo*, 148 F.3d at 591; *Henry Filters, Inc.*, 505 F.3d at 524; *Koch*, 625 F.3d at 479; *Manning*, 738 F.3d at 943 *Mazyak*, 650 F.2d at 792. Other victim statements will be referenced or offered merely to explain why law enforcement took certain investigative actions, and to explain why the email addresses, IP addresses, and phone numbers the victims used to communicate with the criminals could not be used to help identify the defendants. *See U.S. v. Warman*, 578 F.3d 320, 346 (6th Cir. 2009) ("evidence that is 'provided merely by way of background' or is offered only to 'explain[ ] how certain events came to pass or why the officers took the actions they did,' is not offered for the truth of the matter asserted.") (quoting *United States v. Cromer*, 389 F.3d 662, 676 (6th Cir. 2004)); *see also United States v. Powers*, 500 F.3d 500, 508 (6th Cir. 2007) ("testimony provided merely by way of background,

or to explain simply why the Government commenced an investigation, is not offered for the truth of the matter asserted and, therefore, does not violate a defendant's Sixth Amendment rights").

Context for Admissible Statements. Finally, statements only offered to provide context for admissible statements are not hearsay. Thus, for example, where a member of the conspiracy communicated with a victim or other third-party, the victim or other third-party's statements may be offered "to provide context to [the] party admissions." *United States v. Jacob*, 377 F.3d 573, 581 (6th Cir. 2004); *see also United States v. Henderson*, 626 F.3d 326, 337 (6th Cir. 2010) ("the statements made by others were not admitted to show the truth of the matters asserted, but to provide context for Henderson's admissions"); *United States v. Valenzuela*, 88 F. App'x 909, 913 (6th Cir. 2004) (third-party's side of the conversation were not hearsay because they were offered "only to provide context for the damning admissions made by the defendant and by his co-conspirator."); *United States v. Mays*, 69 F.3d 116, 121 (6th Cir. 1995) (purchasers comments about whether defendants added sugar to their products were not hearsay because they were merely providing context to defendants' denials).

2. Even if Offered for The Truth, The Statements Would Also Be Statements of a Party Opponent and in Furtherance of the Conspiracy

With the possible exception of the "victim statements" referenced above, even if the Court found that all of the statements referenced in Section II(B) were statements offered for the truth of the matter asserted, all of these "statements" would be admissible as statements made by the Bayrob Group in furtherance of the conspiracy. FRE 801(d)(2)(E). Where a particular statement can also be attributed to one of the three defendants, the statement is also a statement of a party opponent. FRE 801(d)(2)(A).

The United States already addressed the issue of co-conspirator statements in its March 23, 2013 filing (Dkt. 58), but three points are important to note here: (a) a grand jury already found the existence of the alleged conspiracy and that each defendant was a member; (b) a Romanian court was required to make a similar finding to extradite the defendants; and (c) under well-established Sixth Circuit law, this Court may admit the co-conspirator statements at trial "subject to later demonstration of their admissibility by a preponderance of the evidence." *See United States v. Vinson*, 606 F.2d 149, 152–53 (6th Cir. 1979). While the Court retains the option of holding a "mini-hearing" prior to trial on the issue, that procedure "has been criticized as burdensome, time-consuming and uneconomic." *Id.*

3. The United States May Offer Discrete Categories of Documents Pursuant to the Business and Public Records Exception

The United States may offer the discrete categories of documents below pursuant to the business and public records exception to the hearsay rule. *See* FRE 803(6) ("Records of Regularly Conducted Activity"), FRE 803(8) ("Public Records"). As noted above, these records are not testimonial because they were "created for the administration of an entity's affairs and not for the purpose of establishing or proving some fact at trial." *Melendez-Diaz*, 557 U.S. at 324 (2009).

- Certified Trademark Registrations from the USPTO: The government has already produced to defense copies of all of these certificates currently in its possession. If it obtains additional certified registrations, it will timely produce them to the defense. These registrations are public records and do not raise Confrontation Clause issues because they are not testimonial. *Melendez-Diaz*, 557 U.S. at 324.

- Tiberiu Danet's Certified Visa Application: The government has already produced a copy of the certified visa application to defense. Danet's visa application, another public record, does not raise Confrontation Clause issues because it is not testimonial. *Id.* Danet's statements within his certified visa application are statements of a party opponent. *See* FRE 801(d)(2)(A).

- Provider Records Already Ruled On: The Court already ruled on the government's motion to admit certain records certified pursuant to FRE 902(11) & 902(13). (Dkt. 70.) Miclaus did not file any response to the government's motion and it is too late for Miclaus to revisit this issue now. As the government previously noted, however, "the government is *not* arguing that the *content* of defendants' communications themselves fit into the *hearsay exception* for business records." (Dkt. 60 at 7.) Any content will be offered as non-hearsay, or pursuant to a non-testimonial hearsay exception.

  Law Enforcement Inventories / Chain of Custody Forms: The government has already produced inventory and chain of custody forms created by law enforcement, which are public records. If the government obtains additional forms, it will promptly produce them. Given the Court's prior ruling (Dkt. 70 at 5), the government will treat such evidence as though it *is* testimonial and either (a) offer such evidence through testimony of a live witness involved in the preparation of the form or; (b) only offer the document to the Court to assist in ruling on *prima facie* authenticity under FRE 104. *See, e.g.*, *United States v. Pierce*, 62 F.3d 818, 827 (6th Cir. 1995) ("The Supreme Court held that a district court can consider 'any evidence whatsoever, bound only by the rules of privilege,' to make factual determinations under Rule 104.") (quoting *Bourjaily v. United States*, 483 U.S. 171, 178 (1987).)

In sum, because virtually all of the "statements" in this case will be offered for a non-hearsay purpose, and would also constitute co-conspirator statements (and, in some cases, statements of a party opponent), the government does not foresee hearsay or Confrontation Clause issues at trial. While it is possible that other hearsay exceptions might arise (e.g., "past recollection recorded" if a witness fails to recollect something he or she recorded), the government presently does not foresee relying on any other hearsay exceptions.

C. Authentication

The discussion below is intended to explain how the government may use FRE 901(b)(4) ("distinctive characteristics") to make a *prima facie* showing of authenticity for four particular categories of evidence at trial without providing a complete chain of custody *and without running afoul of the Confrontation Clause*. These four categories of evidence are: (a) digital devices (i.e., cellphones and computers) seized in Romania; (b) audio files from telephone

surveillance in Romania; (c) intercepts of defendants' home internet traffic in Romania; and (d) screenshots of public websites.

1. The Court may Consider Admissible and *Inadmissible* Evidence to Assess Admissibility

The Court must decide preliminary questions about whether evidence is admissible, including whether that evidence is authentic. FRE 104(a). "In so deciding, the court is not bound by evidence rules, except those on privilege." *Id.* "The Supreme Court held that a district court can consider 'any evidence whatsoever, bound only by the rules of privilege,' to make factual determinations under Rule 104." *Pierce*, 62 F.3d at 827 (quoting *Bourjaily*, 483 U.S. at 178.) Thus, in deciding whether evidence is *prima facie* authentic, for example, "the judge may consider . . . hearsay evidence which the jury could not consider." *United States v. Vinson*, 606 F.2d 149, 153 (6th Cir. 1979); *see also, e.g.*, *United States v. Kilpatrick*, No. 10-20403, 2012 WL 3236727, at *5 (E.D. Mich. Aug. 7, 2012) ("This Court can consider the admissions made by Defendant . . . and his attorneys in other proceedings to determine whether the government has made a prima facie showing of authenticity.")

2. The Government Need Only Make a *Prima Facie* Showing of Authenticity

"To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." FRE 901(a). "This burden [under Rule 901] is slight." *United States v. Demjanjuk*, No. 1:99CV1193, 2002 WL 544622, at *21 (N.D. Ohio Feb. 21, 2002), *supplemented*, No. 1:99CV1193, 2002 WL 544623 (N.D. Ohio Feb. 21, 2002), and *aff'd*, 367 F.3d 623 (6th Cir. 2004). "[T]here need only be a *prima facie* showing, to the court, of authenticity, not a full argument on admissibility." *Id.*; *see also United States v. Fluker*, 698 F.3d 988, 999 (7th Cir. 2012 ("Only a prima facie showing of genuineness is required; the task of

deciding the evidence's true authenticity and probative value is left to the jury."); Hon. Paul Grimm, Gregory Joseph & Daniel Capra, *Best Practices for Authenticating Digital Evidence*, pp. 2-3, West Academic Publishing (2016) (describing the roles of the trial court and jury).

"Once a prima facie case is made, the evidence goes to the jury and it is the jury who will ultimately determine the authenticity of the evidence, not the court." *United States v. Thomas*, 921 F.2d 277 (6th Cir. 1990) (citations omitted). "The only requirement is that there has been substantial evidence from which they could infer that the document is authentic." *Id.*; *see also United States v. Carriger*, 592 F.2d 312, 316 (6th Cir. 1979) (concluding "that the district court erred in requiring further authentication of the promissory notes")

3. Chain of Custody Evidence Is Not Required to Authenticate Evidence

"Chain of custody" evidence is just one way to authenticate evidence and is especially important for evidence such as narcotics, which tend to be non-distinct. *See United States v. Cardenas*, 864 F.2d 1528, 1531 (10th Cir. 1989) ("Cocaine, [which is] not uniquely identifiable, requires a sufficient chain of custody to support its admission."). But chain of custody evidence "is merely one possible means of authentication and not . . . an exclusive requirement." *United States v. Browne*, 834 F.3d 403, 411–15 (3d Cir. 2016); *United States v. Camuti*, 78 F.3d 738, 743 (1st Cir. 1996) ("Chain of custody is one means of authenticating evidence but not the only means"); *United States v. Mendel*, 746 F.2d 155, 166 (2d Cir. 1984) (chain of custody evidence is only "one form of proof sufficient to support a finding that the matter in question is what its proponent claims."), *cert. denied*, 469 U.S. 1213 (1985). Rather, "[t]he government may authenticate a document solely through the use of circumstantial evidence, including the document's own distinctive characteristics." *United States v. Smith*, 918 F.2d 1501, 1510 (11th Cir. 1990).

Even where the government relies entirely on chain of custody evidence, "the government need not prove a perfect chain of custody." *United States v. Fried*, 881 F.2d 1077 (6th Cir. 1989). Similarly, "[t]here is no rule that the government must provide the testimony of all of the persons who have had custody of the evidence." *Id.* "Gaps in the chain affect the weight of the evidence and not its admissibility." *Id.*; *see also United States v. Knowles*, 623 F.3d 381, 386 (6th Cir. 2010) ("challenges to the chain of custody go to the weight of the evidence, not its admissibility.") (quoting *United States v. Levy*, 904 F.2d 1026, 1030 (6th Cir. 1990)); *United States v. Combs*, 369 F.3d 925, 938 (6th Cir. 2004) (same).[2]

4. Evidence can be Authenticated Based on "Distinctive Characteristics"

If your cellphone was found on the grass in a remote field and could be unlocked, there is no doubt that the finder would be able to definitively determine it was yours, even if you were nowhere to be found. There would likely be hundreds of emails on the phone, all sent to your email account(s). The phone would likely contain hundreds of photos of you and your friends, and family. There would be contact information in the phone relating to you, your friends, and family. There would likely be texts, chats, and social media profiles, all relating to you. The phone number associated with the phone and the location information on the phone would also connect to you. In short, it would take little effort to definitively confirm that you were the owner of the cellphone.

[2] Similarly, the mere "possibility of tampering or misidentification" is not a basis for a court to preclude the admission of evidence. *Knowles*, 623 F.3d at 386 ("A party must do more than merely raise the possibility of tampering or misidentification to render evidence inadmissible."); *Combs*, 369 at 938 ("Merely raising the possibility of tampering or misidentification is insufficient to render evidence inadmissible."); *United States v. Faulks*, 149 F.3d 1185 (6th Cir. 1998) (same).

This is the fundamental premise behind Federal Rule of Evidence 901(b)(4) which indicates that evidence may be authenticated based entirely on its "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." Fed. R. Evid. 901(b)(4). The Sixth Circuit has regularly affirmed the authentication of evidence based on its distinctive characteristics and other circumstances.

For example, in *United States v. Brown*, 801 F.3d 679 (6th Cir. 2015), the Sixth Circuit held that a drug ledger was properly authenticated based on other objects found near the ledger, associated with the defendant. In *United States v. Shrout*, 298 Fed. Appx. 479 (6th Cir. 2008), the Sixth Circuit found that a planner was properly authenticated based on the consistent placement of name and address across a planner and entries that reflected information independently known about the planner user's business practices and daily activities. And in *United States v. Jones*, 107 F.3d 1147, 1150 (6th Cir. 1997), the Sixth Circuit held that evidence can be authenticated where it "deals with a matter sufficiently obscure or particularly within the knowledge" of the purported author, and found that a card properly authenticated based on references to the defendant's daughter and granddaughter.

5. Foreign Evidence Must Frequently Be Authenticated Based on "Distinctive Characteristics"

For foreign evidence, establishing authenticity via an unbroken chain of custody "would be an impossible standard." *See United States v. Collins*, 715 F.3d 1032, 1035-36 (7th Cir. 2013) (approving admission of audio tapes created in Mexico based on voice identification and distinctive characteristics of the recordings). As a result, evidence obtained from outside of the United States is also frequently authenticated under Rule 901(b)(4) without showing a complete chain of custody. *Id.*; *see also United States v. Dumeisi*, 424 F.3d 566, 574-75 (7th Cir. 2005) (finding a file from Saddam Hussein's former Iraqi Intelligence Service was properly authenticated based on "distinctive characteristics" of the documents themselves, "including the

style and form of the documents" as well as the circumstances relating to the file recovery); *Xiao Wei Yang Catering v. Inner Mongolia, Inc.*, 2017 WL 507211 (D. Mass. 2017) (Chinese government screenshots authenticated based on substance and internal patterns). When chain of custody evidence is used to authenticate foreign evidence, courts may consider the chain of custody beginning when U.S. authorities first receive the evidence. *See Collins*, 715 F.3d at 1035-36 ("We acknowledge that Flores did not testify at trial and that no government agents were present when Flores made the recordings" in Mexico but noting that the recordings "never left the government's possession after the moment of receipt").

In *United States v. Dumeisi*, a Chicago-area man was convicted of acting as an unregistered agent of Saddam Hussein's government based in part on documents found in a foreign country. *See* 424 F.3d 566. At trial, the government introduced the "Baghdad file," a collection of Iraq Intelligence Service (IIS) documents recovered after the 2003 fall of Baghdad. *Id.* at 571-572. Dumeisi challenged the provenance of the Baghdad file. The Seventh Circuit found that the circumstances and the content—which contained certain codes, symbols, and abbreviations that were idiosyncratic to the IIS—sufficed to authenticate the file under FRE 901(b)(4). *Id.* at 575.

In *United States v. Elkins*, 885 F.2d 775 (11th Cir. 1989), Elkins was charged with scheming to sell restricted aircraft to Libya, a prohibited country. The Eleventh Circuit found that several letters found in West Germany in a briefcase allegedly owned by another scheme participant were properly authenticated in light of the contents, the apparent authorship, and other circumstances. *Id.* at 785.

In *United States v. Vidacak*, 553 F.3d 344 (4th Cir. 2009), Vidacak was accused of lying to immigration authorities regarding his military service in the Bosnian Civil war. *Id.* at 347.

Part of the government's proof was military personnel records recovered from the Zvornik Brigade headquarters showing that Vidacak was a member of the Army of the Republika Srpska. Although the person who recovered records in the former Yugoslavia could not explain the pre-seizure history of the information, the Fourth Circuit approved the admissibility of the records in part based on the internal patterns and distinctive characteristics of the military records. *Id.* at 350-351.

The *Dumeisi, Elkins,* and *Vidacak* cases show that FRE 901(b)(4) frequently applies where physical evidence is obtained outside the United States. Such evidence may be authenticated regardless of "chain of custody" and based solely on its distinctive characteristics.[3]

6. Electronic Evidence Frequently Contains "Distinctive Characteristics" That Makes FRE 901(b)(4) "One of the Most Frequently Used" Rules to Authenticate Digital Evidence

As is well illustrated by the example of a lost cellphone found in a field, electronic evidence will often contain distinctive characteristics, some of which are readily observable (like a nickname typed into an email), and some of which require the use of forensic tools (like a hash algorithm). As a result, the nature of electronic evidence provides a unique ability to understand that an item is what the proponent claims it to be. In *Lorraine v. Markel,* then District of Maryland U.S. Magistrate Judge Paul W. Grimm—now a Maryland U.S. District Court Judge—wrote a comprehensive analysis of the admissibility of electronic evidence. *Lorraine,* 241 F.R.D. at 538-585. The *Lorraine* opinion correctly describes FRE 901(b)(4) as "one of the most frequently used [rules] to authenticate email and other electronic records." *Id.* at 546-548); *Best Practices for Authenticating Digital Evidence* at 8. Time has proven District Court Judge

[3] The government anticipates additional testimony of U.S. law enforcement officers present at the time of the seizure of such electronic evidence in Romania, and testimony regarding its being placed into U.S. custody shortly thereafter.

Grimm correct. Indeed, courts have repeatedly upheld the admission of computers and other electronic evidence, even in the absence of chain-of-custody evidence, based solely on identifying evidence found on item itself.[4]

Consistent with the lost cellphone in a field example, in *United States v. Reed*, the Fourth Circuit held that that "the government proffered evidence that the jury could use to attribute" a particular phone to defendant Dyer, despite offering "no testimony about how this phone was seized," because there was evidence of "photos of Dyer on the phone and text messages attributing the number to Dyer, including several that used … his first name." 780 F.3d 260, 265-67 (4th Cir. 2015); *see also United States v. Lewisbey*, 843 F.3d 653, 658 (7th Cir. 2016) (cellphones authenticated, in part, by information on the phones themselves such as "properties," "contacts," and communications associated with the defendant); *United States v. Siddiqui,* 235 F.3d 1318, 1322–23 (11th Cir. 2000) (email authenticated by the use of the defendant's email

[4] *See, e.g., United States v. Browne*, 834 F.3d 403, 408-416 (3d Cir. 2016) (Facebook chat records authenticated based on circumstantial evidence including existence of biographical details of defendant in the chat records); *United States v. Brinson,* 772 F.3d 1314, 1320 (10th Cir. 2014) (Facebook messages authenticated under FRE 901(b)(4) where account was linked to a known email address and defendant used own name in postings); *United States v. Siddiqui,* 235 F.3d 1318, 1322-23 (11th Cir. 2000) (email authenticated by circumstantial evidence, including the presence of the defendant's work email address, content of which the defendant was familiar with, use of the defendant's nickname, and testimony by witnesses that the defendant spoke to them about the subjects contained in the email); *United States v. Tank,* 200 F.3d 627, 630-31 (9th Cir. 2000) (chat log authenticated where it contained the defendant's known screen name); *United States v. Bertram,* No. 3:15-cr-14-GFVT-REW, 2017 WL 1375184, *1-2 (E.D. Ky. April 14, 2017) (emails authenticated based on email addresses and content unique to communication participants); *United States v. Benford,* No. CR-14-321-D, 2015 WL 631089, at *5-6 (W.D. Okla. Feb. 12, 2015) (text messages authenticated because they related information uniquely tied to the defendant); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1153-54 (C.D. Cal. 2002) (admitting printed website postings based on circumstantial indicia of authenticity as website postings belonging to defendant, including dates and presence of identifying web addresses); *Tienda v. State*, 358 S.W.3d 633, 647 (Tex. Crim. App. 2012) (MySpace posts authenticated because defendant used his nickname on account, his photograph was associated with the account, and posts revealed facts that the defendant would know).

address and nickname, as well as its contents which included information the defendant would know); *United States v. Fluker*, 698 F.3d at 999-1000 (7th Cir. 2012) (same); *Koch*, 625 F.3d at 479–80 (affirming the admission of documents where they were used as "circumstantial evidence associating [the defendant] with the computer and flash drive"); *Manning*, 738 F.3d at 943 (finding chats were "circumstantial evidence connecting [defendant] to the child pornography on the computer and [to] the Memorex disc discovered near the computer").

In *State v. Gibson*, 2015 WL 1962850 (6th Cir. 2015), the Sixth Circuit found that a Facebook account was properly authenticated under FRE 901(b)(4) where the distinctive characteristics and circumstances sufficed to show that the account was genuine. The Court was able to make this determination based on terms used in profile, gang names, gang affiliations, and consistent location information.

In *Fluker*, 698 F.3d at 999–1000, the Seventh Circuit found that electronic evidence—a set of emails—was properly authenticated under FRE 901(b)(4) where the distinctive characteristics and circumstances sufficed to show that the emails were genuine. In *Fluker*, the email address indicated that the email was sent by a member of "MTE," a business organization used by conspirators, and the email contents demonstrated that the sender possessed information that only a scheme "insider" would know. *Id.*

Two fairly recent cases explore the volume and comprehensive nature of electronic evidence, *Riley v. California*, __ U.S. __, 134 S. Ct. 2473 (2014) and *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (*en banc*). Although neither case involves the admissibility of electronic evidence, both explain how electronic evidence provides unusual insight into who used the device and when, where, and how the device was used. When the distinctive characteristics of information found in a device answer the "who, what, where, and how" about a

device, sufficient evidence exists for a finding that the device is what its proponent claims it to be.

In *Riley*, the Court rejected searches of cell phones incident to arrest and made clear that search warrants are required for cell phones found on an arrestee. *Riley*, 134 S. Ct. at 2485. In doing so, the *Riley* opinion explored how the characteristics of "smart" phones provide extraordinary insight into a person's life in light of the volume and types of information stored in a cell phone. *Id.* at 2489. The Court observed that a cell phone may contain bank information, addresses, calendars, contact lists, still and video depictions, notes, detailed communication records, internet search and browsing histories, geolocation information, and software application downloads and use histories. *Id.* at 2489-90. Further, the Court observed, cell phone information allows a forensic examiner to "reconstruct" an individual's life through "a thousand photographs labeled with dates, locations, and descriptions." *Id.* at 2489. That information, when placed in chronological and geographic context of other information within the device, "reveal[s] much more in combination than any isolated record." *Id.* Moreover, the Court opined that digital data, like internet search and browsing history, is often unique in its ability to "reveal an individual's private interests or concerns." *Id.* at 2490.

In *United States v. Ganias*, the *en banc* Second Circuit overruled an earlier panel decision that had held that law enforcement lacked good faith in executing a 2006 search warrant against computer evidence first secured in 2003 in a different investigation. The panel decision had suppressed evidence from the 2006 search holding that the investigators in the original case should have segregated and extracted only the pertinent information relating to the first target and that it was error to retain additional information. *United States v. Ganias*, 755 F.3d 125, 138-40 (2d Cir. 2014).

In overruling the original decision, the *en banc* Second Circuit largely rejected the central analogy used the panel decision—that computer records are like documents stored in a filing cabinet. *Ganias,* 824 F.3d at 211-12. In contrast, the *en banc* opinion noted that a single computer file may be stored in a fragmented way, and with unseen redundancies, on the storage medium. *Id*., at 212-13. The Second Circuit noted that a "digital storage device . . . is a coherent and complex forensic object" (*id.* at 213) and the "complexity of the data thereon" may influence subsequent authentication of the device at trial. (*Id.* at 215).

In addressing privacy concerns, the Second Circuit referenced *Riley* while observing that information stored in an electronic device may provide unusual insight into the user's identity, actions, thoughts, and location. *Id*. at 218 (citing *Riley*, 134 S.Ct. at 2489–90). The *en banc* Second Circuit also cited *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013), in which the Circuit noted that "advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain." *Ganias,* 824 F.3d at 218.

Riley and *Ganias* concern Fourth Amendment privacy interests in electronically stored information. While the scope of information on an electronic device can raise privacy concerns, a real world analogy provides perspective: in drug or firearm possession cases, trial courts regularly allow litigants to introduce evidence that is indicia of occupancy or control (*e.g.*, a driver's license, photographs, prescription medication, or correspondence) which tends to show who lived where contraband was found. *See, e.g., United States v. Pulido-Jacobo,* 377 F.3d 1124, 1132 (10th Cir. 2004) (finding a receipt to be admissible non-hearsay because "the government offered the engine receipts only to show that [defendant] had sufficient control of the car to store an old receipt in it."); *United States v. Mazyak*, 650 F.2d 788, 792 (5th Cir. 1981)

("The letter was not introduced to prove the truth of the matter asserted; rather, it was introduced as circumstantial proof that the appellants were associated with each other and the boat.").

Applying the same idea to electronically stored information, the content, volume, variety, and complexity of electronically stored information can show the "who, what, when, where, and how" of computer use in connection with a crime.

7. The United States May Authenticate Digital Evidence Based Primarily on Distinctive Characteristics

Below is a summary of the evidence the United States may seek to admit, in part, through distinctive characteristics, pursuant to FRE 901(b)(4). Because the testimony of a multiple witnesses will likely support the admission of each item, the United States anticipates that several witnesses may identify and discuss a particular piece of evidence before the United States requests that it be admitted into evidence.

Digital Devices. The United States will seek to admit a number of digital devices seized from the defendants' person or residence, including cellphones, computers, storage devices, and a directional antenna. The United States will present a *prima facie* case of authenticity with respect to these devices primarily based on testimony regarding (a) files and artifacts (e.g., pictures, emails, contacts, account information, word documents) in each of these devices that tend to show who controlled the device; (b) consistent information or files in different devices controlled by the same defendant (e.g., the same email account set up on multiple phones owned by the same defendant), and (c) testimony regarding metadata showing that the files and artifacts arrived on the digital device prior to each defendant's arrest. *See, e.g.*, *Reed*, 780 F.3d at 265-67 ("the government proffered evidence that the jury could use to attribute" a particular phone to defendant Dyer, despite offering "no testimony about how this phone was seized," because there was evidence of "photos of Dyer on the phone and text messages attributing the number to Dyer,

including several that used … his first name."): *Lewisbey*, 843 F.3d at 658 (cellphones authenticated, in part, by information on the phones themselves such as "properties," "contacts," and communications associated with the defendant); *Koch*, 625 F.3d at 479–80 (affirming the admission of documents where they were used as "circumstantial evidence associating [the defendant] with the computer and flash drive," not to show that the defendant authored the documents).

Audio Files. The United States will seek to admit one or more audio files, reflecting telephone surveillance on Defendant Bogdan Nicolescu's home telephone pursuant to an MLAT request by the United States. The United States will present a *prima facie* case of authenticity with respect to these audio files based primarily on "voice identification" by testimony from someone already familiar (and/or who has become familiar) with Nicolescu's voice, as well as distinctive characteristics regarding what was discussed in the call itself (e.g., the domain name that the defendants' used for their secure Jabber server in Danet's residence, and a nickname used by Nicolescu). *See United States v. Simms*, 351 F. App'x 64, 69 (6th Cir. 2009) ("the Federal Rules of Evidence allows voice identification by someone who became familiar with the voice *at any time* and does not place a time limitation on the familiarity"); *United States v. Cooke*, 795 F.2d 527, 530 (6th Cir. 1986) ("[t]he standard for the admissibility of an opinion as to the identity of the speaker is merely that the identifier has heard the voice of the alleged speaker at any time."); *Collins*, 715 F.3d at 1035-36 (approving admission of audio tapes created in Mexico based on voice identification and distinctive characteristics of the recordings).

Intercepts of Defendants' Home/Cellular Internet Traffic. The United States may offer one or more electronic file, reflecting intercepted internet traffic from defendants' residences (so called, "packet capture," or "PCAP files"). The United States will present a *prima*

facie case of authenticity with respect to these PCAP files based primarily on distinctive characteristics from the PCAP files showing (a) that they are PCAP files from the relevant date and time; (b) that they correlate with data produced and authenticated by U.S. providers; and (c) they relate to each defendant (e.g., data showing a defendant logging onto his personal email account and using the password associated with that account). *See, e.g., Fluker*, 698 F.3d at 999 (e-mails authenticated in part based on distinctive characteristics of the emails themselves); *Siddiqui*, 235 F.3d at 1322 (email was properly authenticated as having been authored by defendant where it bore defendant's email address, a reply automatically was directed to defendant's email address, and the content of the email referred to matters known to defendant); *U.S. E.E.O.C. v. Olsten Staffing Services Corp.*, 657 F. Supp. 2d 1029 (W.D. Wis. 2009) ("e-mails may be authenticated through the e-mail addresses in the headers and other circumstantial evidence, such as the location where the e-mail was found").

Screenshots of Public Webpages: The United States will seek to admit several public webpages based on (a) testimony from a witness that the screenshot represents a fair and accurate screen capture of the webpage as of the time the witness visited the website; and (b) distinctive characteristics of the webpage linking the page either to one of the defendants and/or to the Bayrob Group's criminal scheme. *See, e.g., Gibson*, 2015 WL 1962850 (6th Cir. 2015) (finding Facebook page was properly authenticated under FRE 901(b)(4) and noting "courts consider evidence from all sources (even if not from a live witness)—including documents, whether electronic or hard copy—on a continuum. That is, clearly authentic evidence is admitted, clearly inauthentic evidence is excluded, and everything in between is conditionally relevant and admitted for the jury to make the final determination of authenticity."); *Browne*, 834 F.3d 408-416 (Facebook chats authenticated based on circumstantial evidence including

existence of biographical details of defendant in the chat records); *Xiao Wei Yang Catering*, 2017 WL 507211 (Chinese government screenshots authenticated based on substance and internal patterns); *Perfect 10, Inc.*, 213 F. Supp. 2d at 1153-54 (screenshots from websites authenticated by circumstantial indicia that the website postings belonged to defendant, including dates and presence of identifying web addresses); *Tank*, 200 F.3d at 630-31 (chat room log authenticated because it contained the defendant's known screen name); *Benford*, No. CR-14-321-D, 2015 WL 631089, at *5-6 (W.D. Okla. Feb. 12, 2015) (text messages authenticated because they related information uniquely tied to the defendant); *Tienda*, 358 S.W.3d 633, 647 (Tex. Crim. App. 2012) (MySpace posts authenticated because defendant used nickname on account, his photograph was associated with the account, and posts revealed facts that the defendant would know).

In short, the United States intends to present its evidence at trial in a manner that will not raise evidentiary or constitutional concerns.

CONCLUSION

As discussed at great length, the United States does not presently intend to introduce any testimonial hearsay statements, or any statements pursuant to FRE 807 (the "residual exception"). In addition to meeting its discovery obligations, at Miclaus' request, the United States has already (1) produced its hot documents; (2) met in person on multiple occasions to discuss those documents; and (3) provided trial exhibits, practically as they are created. The United States will continue to do so. The United States has also provided lengthy explanations as to why the admission of these documents will not cause evidentiary or constitutional concerns. *See* Dkt. 58, 60, and *supra*. Miclaus has identified no reason for the Court to deviate from the existing pretrial order. Miclaus' motion should be denied.

Respectfully submitted,

JUSTIN E. HERDMAN
United States Attorney

By: /s/ Duncan T. Brown

Duncan T. Brown (NY: 3982931)
Assistant United States Attorney
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3933
(216) 522-7499 (facsimile)
Duncan.Brown@usdoj.gov

Brian L. Levine (DC: 480216)
Senior Counsel
United States Department of Justice
1301 New York Avenue, Suite 600
Washington, DC 20005
(202) 616-5227
(202) 514-6113 (facsimile)
Brian.Levine@usdoj.gov

Brian M. McDonough (OH: 0072954)
Assistant United States Attorney
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3965
(216) 522-2403 (facsimile)
Brian.McDonough@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on this 6th day of July, 2018, a copy of the Opposition to Miclaus' Motion in Limine Re: Testimonial Hearsay Statements was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/ Duncan Brown
Duncan T. Brown
Assistant United States Attorney